REMARKS

The Examiner has rejected Claims 1, 4, 7-8, 11, 14-15, 18 and 21 under 35 U.S.C. 102(b) as being anticipated by Arnold (U.S. Patent No. 5,440,723). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to each of the independent claims.

With respect to the independent claims, the Examiner has relied on Col. 29, lines 36-38; Col. 23, lines 23-33; Col. 24, lines 21-26; and Col. 23, lines 40-45 from the Arnold reference to make a prior art showing of applicant's claimed technique "wherein said warning generating logic can generate a plurality of different types of warnings to said user that said target computer file may have suffered irreparable damage and said library includes data specifying which of said plurality of types of warnings should be issued in response to a particular detected computer virus" (see this or similar, but not necessarily identical language in the independent claims - as amended).

In addition, the Examiner has argued that "'if VIRSCAN fails to identify any of the changes to the executables as a known virus would make', as taught by Arnold, is equivalent to that the target computer file may have suffered irreparable damage caused by the virus since the changes can not be identified and thereby the damage has no way to be recovered/repaired." The Examiner has also argued that "all different types of warning is issued depending upon different situations where signature data or copies of any unknown virus is effectively used along with the library test files, as taught by Arnold."

Applicant respectfully points out that the above noted reference citations relied upon by the Examiner merely teach "repair mechanisms designed for specific known types of undesirable software entities" (Col. 29, lines 36-37), that "VIRSCAN employs a database of signatures consisting of byte sequences which are known to be contained in known viruses" (Col. 23, lines 23-25), and that "VIRSCAN is run on all of the changed

executables to determine whether the change can be attributed to a known virus, i.e., one contained in the VIRSCAN signature database"(Col. 23, lines 29-32).

The excerpts from Arnold also teach that in the event of "a failure by VIRSCAN to find another instance of the derived signature... the user receives a warning message to this effect" (Col. 24, lines 23-26) and that "[i]f VIRSCAN fails to identify any of the changes to the executables as a known virus, the user is informed of the situation" (Col. 23, lines 39-41).

However, applicant respectfully asserts that only generally disclosing that "the user receives a warning message" and that "the user is informed of the situation" when "VIRSCAN fails to identify any of the changes to the executables as a known virus," as in Arnold, does not meet "generat[ing] a plurality of different types of warnings," much less a specific technique "wherein said warning generating logic can generate a plurality of different types of warnings to said user that said target computer file may have suffered irreparable damage," as claimed by applicant (emphasis added).

Furthermore, applicant respectfully points out that the use of a database of signatures, along with a plurality of different programs utilized in anti-virus detection (see Col. 22, lines 5-11), as in Arnold, does not meet any sort of a library which "includes data specifying which of said plurality of types of warnings should be issued in response to a particular detected computer virus," as claimed by applicant (emphasis added). For example, Arnold only teaches that a "[i]f VIRSCAN fails to identify any of the changes to the executables as a known virus, the user is informed of the situation" (Col. 23, lines 40-42-emphasis added), and that "[i]f the anomaly is found to be due to a known virus...the user is alerted (see Col. 5, lines 59-61). Clearly, Arnold only distinguishes between alerts for detected known viruses and alerts for identified changes that are not attributed to a known virus, which does not meet applicant's claimed "library [that] includes data specifying which of said plurality of types of warnings should be issued in response to a particular detected computer virus," as claimed by applicant (emphasis added).

Thus, merely disclosing that "VIRSCAN employs a database of signatures consisting of byte sequences which are known to be contained in known viruses," that "the user receives a warning message," and that "the user is informed of the situation" when "VIRSCAN fails to identify any of the changes to the executables as a known virus," as in Arnold, does not meet a "library [that] includes data specifying which of said plurality of types of warnings should be issued," much less a specific technique "wherein said warning generating logic can generate a plurality of different types of warnings to said user that said target computer file may have suffered irreparable damage and said library includes data specifying which of said plurality of types of warnings should be issued in response to a particular detected computer virus," as claimed by applicant (emphasis added).

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.* 868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Arnold reference, as noted above.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to Claim 4 et al., the Examiner has relied on Col. 23, lines 41-42; Col. 24, lines 12-15; and Fig. 3, elements F, J, K, O, and G from the Arnold reference to make a prior art showing of applicant's claimed technique "wherein said warning to said user that said target computer file may have suffered irreparable damage includes an option to add a notification message into said target computer file."

Applicant respectfully asserts that the excerpts relied upon by the Examiner merely teach that "[i]f VIRSCAN fails to identify any of the changes to the executables as a known virus, the user is informed of the situation" (Col. 23, lines 39-41) and that "[i]n a partially manual mode of operation, and at the user's request, the immune system attempts to capture a copy of any unknown virus that might be in the system by using decoy programs" (Col. 23, lines 41-44). The excerpts also teach that "[a] warning message is generated if VIRSCAN fails to find the virus, and a high alert state is entered" (Col. 24, lines 13-15).

Additionally, the excerpts teach running VIRSCAN on changed executables, deploying decoy programs, isolating the viral portion of the modified decoys, adding signatures to a database, and running VIRSCAN on all executables (Fig. 3, elements F, J, K, O, and G).

However, applicant respectfully asserts that informing a user of the existence of an unknown virus, as well as generating a warning message if VIRSCAN fails to find the virus, as in Arnold, only generally suggest sending a warning to a user. Clearly only sending a warning to a user does not suggest adding a notification message into a target computer file, much less a specific technique "wherein said warning to said user that said target computer file may have suffered irreparable damage includes an option to add a notification message into said target computer file," as claimed by applicant (emphasis added).

Again, the foregoing anticipation criterion has simply not been met by the Arnold reference, as noted above. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

With respect to Claim 5 et al., as rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold, in view of Waldin (U.S. Patent No. 6,094,731), the Examiner has relied on the following excerpt from the Waldin reference to make a prior art

showing of applicant's claimed technique "wherein said notification message includes authentication data identifying said target computer file into which it was inserted."

> "...viruses, unequivocally (step 37). If the decrypted transmitted message digest is identical to the calculated message digest, the contents of file 1 are deemed by authentication module..." (Col. 6, lines 65-67)

Applicant respectfully points out that the above excerpt, when read in context, merely teaches that "[i]f the decrypted transmitted message digest is identical to the calculated message digest, the contents of file 1 are deemed by authentication module 12' to be 'unchanged in a way that could allow for a viral infection'" (Col. 6, line 65 – Col. 7, line 2). However, merely determining from a decrypted transmitted message digest that the contents of a file are "unchanged in a way that could allow for a viral infection," as in Waldin, does not even suggest any sort of notification message, much less a technique "wherein said notification message includes authentication data identifying said target computer file into which it was inserted," as claimed by applicant (emphasis added).

With respect to Claim 6 et al., as also rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold, in view of Waldin, the Examiner has relied on the following excerpt from the Waldin reference to make a prior art showing of applicant's claimed technique "wherein said notification message includes an electronic signature applied by said warning generating logic."

> "...respectively identical to all of the pre-stored hash values, authentication module 12' examines the authenticity of digital signature 15 (step 39). This is preferably done via four substeps: 50, 51, 52, and 53. In sub-step 50, authentication module 12' decodes the encoded digital signature 15. In sub-step 51, authentication module 12' decrypts the digital signature 15 using public key 13, producing a decrypted message digest. In sub-step 52, authentication module 12' calculates a new message digest of the contents of critical sectors file 4, using the same message digest algorithm that was used by module 12 of originating computer 2. In sub-step 53, the decrypted message digest is compared with the calculated message digest. If these two numbers do not match, the transmitted data have been changed in some way and the entire contents of file 1 must be rescanned for viruses, unequivocally (step 37). If the decrypted transmitted message digest is identical to the calculated message

digest, the contents of file 1 are deemed by authentication module..." (Col. 6, lines 50-67)

Applicant respectfully asserts that the above excerpt only teaches that "authentication module 12' examines the authenticity of digital signature 15." The above excerpt further teaches that the authentication module "decodes the encoded digital signature," "decrypts the digital signature... producing a decrypted message digest," "calculates a new message digest of the contents of critical sectors file 4," and compares "the decrypted message digest... with the calculated message digest" in order to determine if "the transmitted data have been changed in some way and the entire contents of file 1 must be rescanned for viruses." Further, the above excerpt also teaches that "[i]f the decrypted transmitted message digest is identical to the calculated message digest, the contents of file 1 are deemed by authentication module 12' to be 'unchanged in a way that could allow for a viral infection'" (Col. 6, line 65 – Col. 7, line 2).

Applicant respectfully asserts that decoding an encoded signature, decrypting the signature to produce a decrypted message digest, calculating a new message digest, and comparing the decrypted message digest to the calculated message digest in order to determine if a virus rescan is necessary, as in Waldin, in no way teaches a notification message, much less a technique "wherein said notification message includes an electronic signature applied by said warning generating logic," as claimed by applicant (emphasis added).

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Again, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P503/00.147.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100